HP Select Identity Software

Connector for Netegrity SiteMinder

Connector Version: 3.81

Installation and Configuration Guide

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Select Identity uses software from the Apache Jakarta Project including:

- Commons-beanutils
- Commons-collections
- Commons-logging
- Commons-digester
- Commons-httpclient
- Element Construction Set (ecs)
- Jakarta-poi
- Jakarta-regexp
- Logging Services (log4j)

Additional third party software used by Select Identity includes:

- JasperReports developed by SourceForge
- iText (for JasperReports) developed by SourceForge
- BeanShell
- Xalan from the Apache XML Project
- Xerces from the Apache XML Project
- Java API for XML Processing from the Apache XML Project
- SOAP developed by the Apache Software Foundation
- JavaMail from SUN Reference Implementation
- Java Secure Socket Extension (JSSE) from SUN Reference Implementation
- Java Cryptography Extension (JCE) from SUN Reference Implementation
- JavaBeans Activation Framework (JAF) from SUN Reference Implementation

- OpenSPML Toolkit from OpenSPML.org

- JGraph developed by JGraph

- Hibernate from Hibernate.org

- BouncyCastle engine for keystore management, bouncycastle.org

Trademark Notices

Support

You can visit the HP software support web site at:

http://www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest

- Submit and track support cases and enhancement requests

- Download software patches

- Manage support contracts

- Look up HP support contacts

- Review information about available services

- Enter into discussions with other software customers

- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract.

To find more information about support access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1 Documentation Map

This chapter describes the organization of HP Select Identity connector documentation and provides necessary information on how to use the documentation set to install and configure the connectors.

Figure 1 illustrates the documentation map for Select Identity connector. For a list of available product documentation, refer to the Table 1.

Figure 1   Documentation Map

Table 1   Connector Documentation

Document Title and Filename	Contents	Location
Release Note `SiteMinder Connector v`*3.81* `Release Note.htm`	This file contains necessary information on new features of the connector, enhancements, known problems or limitations, and support information.	`/Docs/` subdirectory under the connector directory.

Connector Deployment Guide (for Select Identity 4.20)
`connector_deploy_SI4.20.pdf`
 	
Connector Deployment Guide (for Select Identity 4.10-4.13)
`connector_deploy_SI4.13.pdf`
 	
Connector Deployment Guide (for Select Identity 4.0-4.01)
`connector_deploy_SI4.pdf`
 	
Connector Deployment Guide (for Select Identity 3.3.1)
`connector_deploy_SI3.3.1.pdf`
	Connector deployment guides provide detailed information on:
	• Deploying a connector on an application server.
	• Configuring a connector with Select Identity.
	Refer to these guides when you need generic information on connector installation.
		`/Docs/` root directory on the product's CD media.

Connector Installation and Configuration Guide `SiteMinder_guide.pdf`	Connector installation and configuration guide provides installation instructions for a specific connector. It contains resource specific configuration details.	`/Docs/` subdirectory under the connector directory.

2 Introduction

This chapter gives an overview of the HP Select Identity connector for Netegrity SiteMinder. An HP Select Identity connector for Netegrity SiteMinder enables you to provision users and manage identities on Netegrity SiteMinder. At the end of this chapter, you will be able to know about:

- The benefits of HP Select Identity.
- The role of a connector.
- The connector for Netegrity SiteMinder.

About HP Select Identity

HP Select Identity provides a new approach to identity management. Select Identity helps you automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. Select Identity communicates with the enterprise information system through connectors, and automates the tasks of identity management. The enterprise information system, which is also referred to as **resource**, can be a database, a directory service, or an ERP package, among many others.

About Connectors

You can establish a connection between a resource and Select Identity by using a connector. A connector is resource specific. The combination of Select Identity and connector helps you perform a set of tasks on the resource to manage identity. A connector can be **unidirectional** or **bidirectional**. A unidirectional connector helps you manage identities from Select Identity, but if any change takes place in resource, it cannot communicate that back to Select Identity. On the other hand, a bidirectional connector can reflect the changes made on resource back to Select Identity. This property of bidirectional connectors is known as **reverse synchronization**.

About the SiteMinder Connector

The connector for Netegrity SiteMinder — hereafter referred to as SiteMinder connector — enables Select Identity to perform the following tasks on Netegrity SiteMinder systems:

- Add, update, and remove users
- Retrieve user attributes

- Enable and disable users

- Verify a user's existence

- Change user passwords

- Reset user passwords

- Retrieve all entitlements

- Retrieve a list of supported user attributes

- Grant and revoke entitlements to and from users

It is a one-way connector and pushes changes made to user data in the Select Identity database to a target Netegrity SiteMinder server and its configured user store (such as Sun ONE DirectoryServer). The mapping file defines how Select Identity fields are mapped to SiteMinder fields.

The SiteMinder connector can be used with Select Identity 3.3.1-4.20.

Overview of Installation Tasks

Before you start installing the connector, you must ensure that system requirements and all the installation prerequisites are met. Refer to the Table 2 for an overview of installation tasks.

Table 2   Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 13.
	— Meet the system requirements.	See System Requirements on page 14.
	— Extract contents of the Schema file (file that contains the mapping files for the connector) to location on the Select Identity server.	See Extracting Contents of the Schema File on page 14.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 14.
	— Cofigure the application server.	See Configuring the Application Server on page 15.
	— Configure SiteMinder	See Configuring SiteMinder on page 16.
2	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 23.

3 Installing the Connector

This chapter elaborates the procedure to install SiteMinder connector on Select Identity server. At the end of this chapter, you will know about

- Software requirements to install the SiteMinder connector.

- Prerequisite conditions to install SiteMinder connector.

- Procedure to install SiteMinder connector.

SiteMinder Connector Files

The SiteMinder connector is packaged in the following files in the `Netegrity Siteminder` directory on the Select Identity Connector CD:

Table 3   SiteMinder Connector Files

Serial Number	File Name	Description
1	• `NetSmConnector_420.rar` for WebSphere • `NetSmConnector_420WL9.rar` for WebLogic	The Resource Adapter Archive (RAR) file contains the connector binaries.
2	`NetSmSchema.jar`	The Schema file contains the mapping files that contain attribute information of Netegrity SiteMinder.

System Requirements

The SiteMinder connector is supported in the following environment:

Table 4   Platform Matrix for SiteMinder connector

Select Identity Version	Application Server	Database
3.3.1	WebLogic 8.1.4 on Windows 2003	Microsoft SQL Server 2000
	WebLogic 8.1.5 on Red Hat Enterprise Linux AS Release 3.0	Oracle 10g
4.0-4.20	The SiteMinder connector is supported on all the platform configurations of Select Identity 4.0-4.20.	

This connector is supported with Netegrity SiteMinder, version 5.5, on Windows 2000 and Solaris 8.

Extracting Contents of the Schema File

The Schema file of the connector contains necessary mapping information to map resource attributes to Select Identity. Extract contents of the NetSmSchema.jar file to a directory that is in the application server CLASSPATH. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instruction to extract contents of the Schema file.

Installing the Connector RAR

To install the RAR file of the connector (such as NetSmConnector_420.rar) on the Select Identity server, you must copy the file to a local subdirectory on the Select Identity server, and then deploy on the application server. Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on deploying a RAR file on an application server.

While deploying the RAR on WebSphere, enter the JNDI Pool Name as
eis/NetSm.

Configuring the Application Server

You must copy SiteMinder Java Application Program Interfaces (API) JAR files to the application server. You must also copy the SiteMinder shared libraries to the application server. These libraries are called by the SiteMinder agent APIs, which are used by the connector for provisioning. After that, you must set the application server's `CLASSPATH` and `LD_LIBRARY_PATH` environment variables to reference the files. Perform the following steps to configure the application server.

1   Create a directory named `SiteMinderConnectorLib` in the Select Identity home directory.

2   Copy the SiteMinder Java API JAR files, which are distributed with SiteMinder, to the `SiteMinderConnectorLib` subdirectory. These files are:

    — `Smjavaagentapi.jar`

    — `Smjavasdk2.jar`

    The default location of these files on the SiteMinder system is `C:\Program Files\Netegrity\SiteMinder\SDK\java\`.

3   Add the JAR files to the application server startup script. Here is an example:

    ```
    set CLASSPATH=%WEBLOGIC_CLASSPATH%;
    %POINTBASE_CLASSPATH%;%JAVA_HOME%\jre\lib\rt.jar;
    %WL_HOME%\server\lib\webservices.jar;
    c:\SelectIdentity\SiteMinderConnectorLib\smjavaagentapi.jar;
    c:\SelectIdentity\SiteMinderConnectorLib\smjavasdk2.jar;
    %CLASSPATH%
    ```

4   Copy the following files to the folder `SiteMinderConnectorLib` subdirectory.

    — `smagentapi.dll`

    — `smjavaagentapi.dll`

    These files can be copied from the SiteMinder system, where they typically reside in `C:\Program Files\Netegrity\SiteMinder\SDK\bin\`.

5   On Solaris, copy the following files to a directory on the server:

    — `libsmagentapi.so`

    — `libsmjavaagentapi.so`

    For the steps 4 and 5, set `PATH` or `LD_LIBRARY_PATH` environment variables appropriately in the WebLogic startup script.

    For example, in the WebLogic startup script, add the following line:

    For .so files:
    **export LD_LIBRARY_PATH=/opt/si/weblogic/sysArchive/
    SiteMinderConnectorLib:$LD_LIBRARY_PATH**

    For .dll files:
    set PATH = C:\Select_Identity\SiteMinderConnectorLib;%PATH%

    Then, set the `LD_LIBRARY_PATH` environment variable to this directory. This environment variable should be available for use by the application server.
    For example, in the WebLogic startup script, locate the following line:

```
export LD_LIBRARY_PATH=/opt/si/weblogic/sysArchive/
SiteMinderConnectorLib:$LD_LIBRARY_PATH
```

On UNIX, use colon (:) to separate library paths. On Windows, use semicolon (;).

Configuring SiteMinder

The SiteMinder connector manages users in SiteMinder using the SiteMinder Java DMS APIs.

In this section, the following configurations are assumed.

- SiteMinder Policy Server 5.5 Service Pack 3 (RC21) and SDK on Solaris 8 or Windows 2000 Server

- SiteMinder WebAgent configured for the following web servers:

  — iPlanet 6.0 on HP-UX11i, Solaris 9, and Windows

  — Microsoft IIS on Windows

- iPlanet Directory Server 5.1 on Solaris 9 or Windows, which acts as the user directory

To configure SiteMinder for use with the connector:

1   Verify that SiteMinder Policy Server and WebAgent are installed and functioning correctly. On the SiteMinder Policy Server, select **Start** → **Program Files** → **SiteMinder** → **SiteMinder Test Tool**.
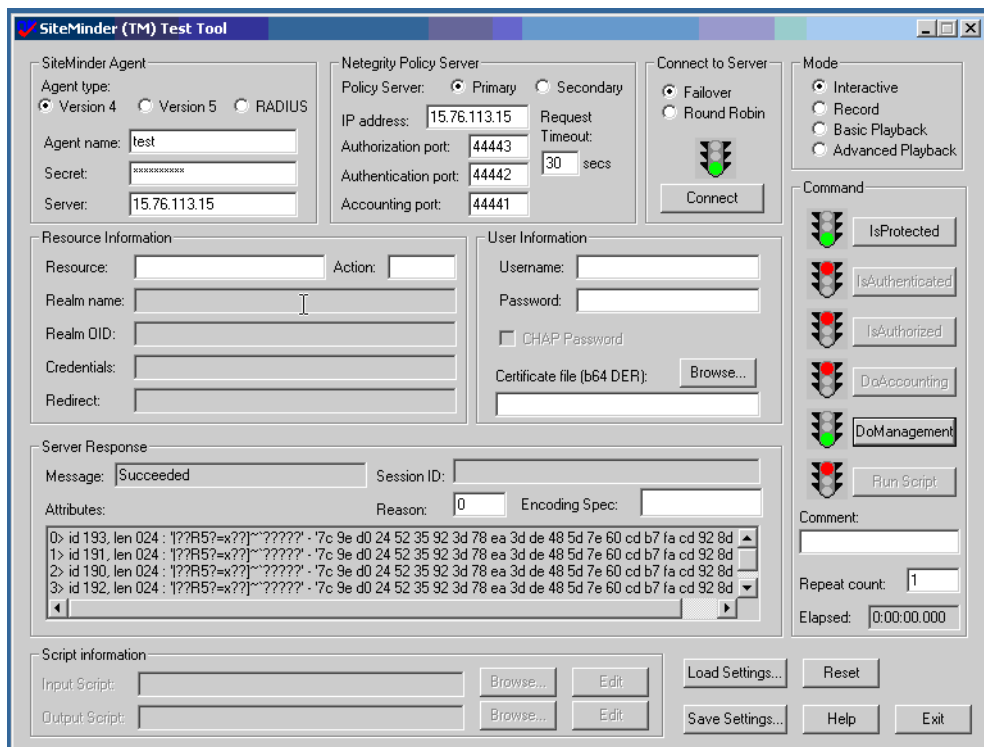
2   Verify that the **Support 4.x agents** option, which is required by the DMS APIs, is selected as shown in the following snapshot. This can be viewed by clicking the agent properties in the SiteMinder user interface.
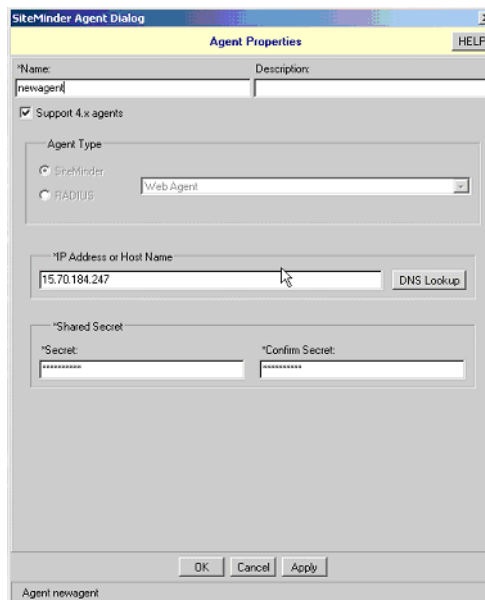
3   To execute the APIs on the Select Identity server, register the Select Identity host system as a trusted host in the SiteMinder Policy Server's database. Complete these steps to do so:

a   Create a Host-Config-Object in the SiteMinder interface and specify the Policy Server IP address there. For example, in the following snapshot, the TestHostConfigObject Host-Config-Object was created by duplicating the default host object and updating the Policy Server information.
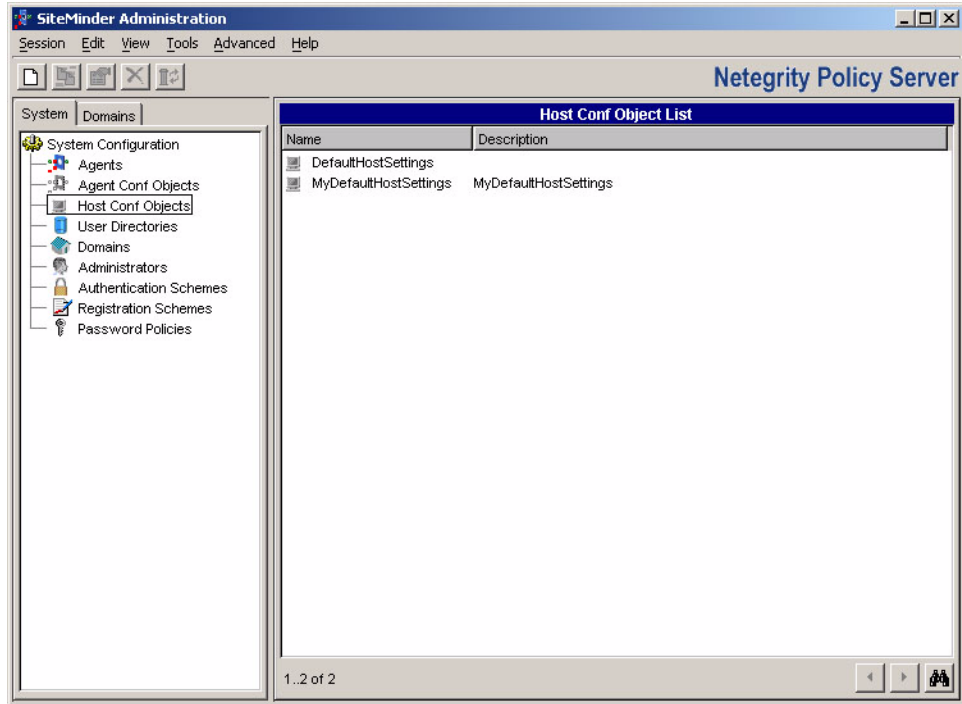
b   Using the `smreghost` utility from an existing WebAgent installation or the WebAgent software, run the utility on the Select Identity server by specifying the Policy Server IP address, SiteMinder administrative login, password, current host name, and the name of the Host-Config-Object that was created above.
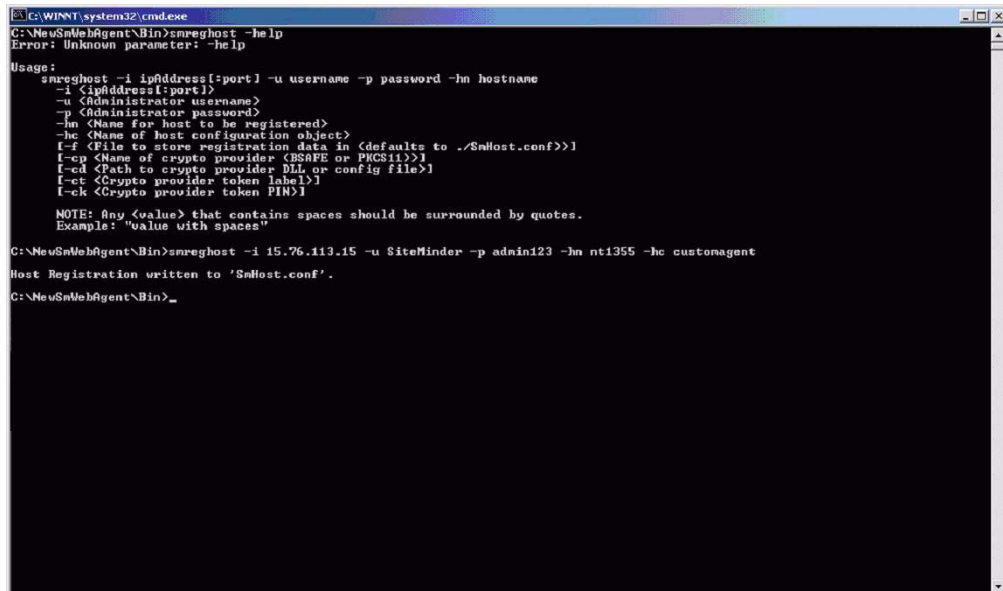
> If the Select Identity server is on a Windows system, use this utility from the Windows WebAgent software. If the Select Identity server is on Linux, use the utility from the Linux WebAgent software.

The output of this command is written to a file called `SmHost.conf`.

4   Locate the `WebAgent.conf` file that was extracted from the `NetSmSchema.jar` file. It typically resides in `SI_home/com/trulogica/truaccess/connector/netSm/`. Update the `WebAgent.conf` file from values in the generated `SmHost.conf` file. Specifically, update the variables for the host name, default agent name, and policy server IP address. Here are example values:

```
hostname="nt1325"
defaultagentname="test"
maxsocketsperport="20"
minsocketsperport="2"
newsocketstep="2"
requesttimeout="10"
policyserver="15.76.113.15, 44441, 44442, 44443"
sharedsecret="{RC2}mLog6JDcu3TzSNE457J+bRdL2QigyQrDbTbevbg4WQz3U
vvbKdyQnoFmuiUCoZp1H/fp7epKZMhEZQP+OBNJJc6OTrCnkvOkpR35Vts5Nnnx
rLhra3B2umee+eDWC3zIKAXJ6sHGWqJgUiMN+PIVlmks9uDSn2HmrUfdLl0FBVBs
Ztjto+vHNXy8eQefhqkr"
```

5 Configure SiteMinder such that it knows the user password attribute name in the configured LDAP User Store.

    a   On the left side of the window, select the configured user store.

    b   Right-click to view the User Directory Properties dialog.
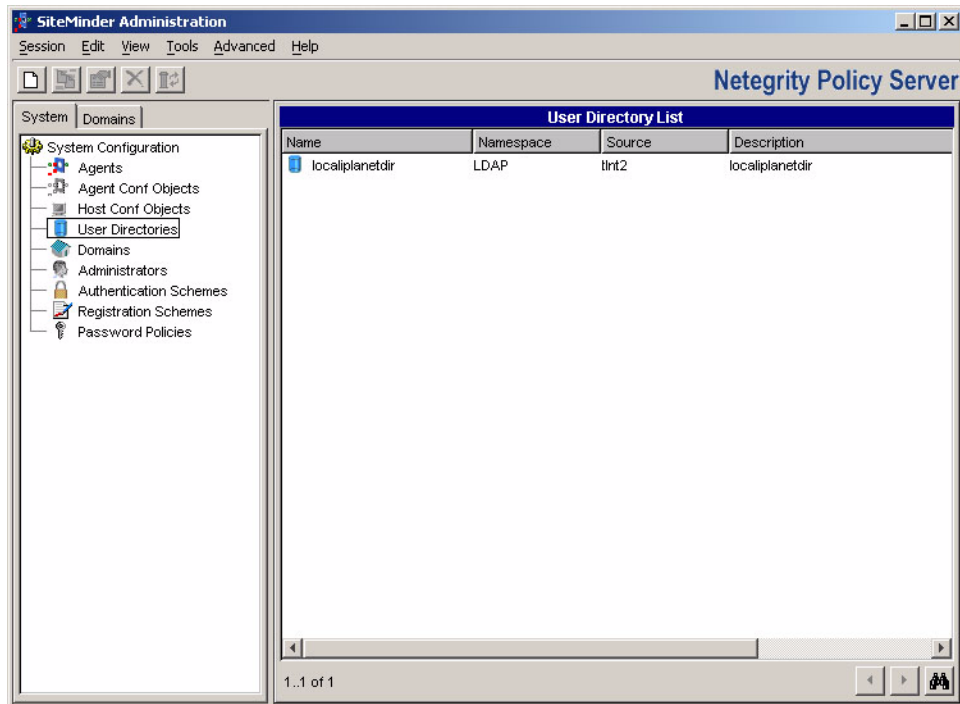
    c   Configure the Directory Setup tab as shown in the following snapshot:
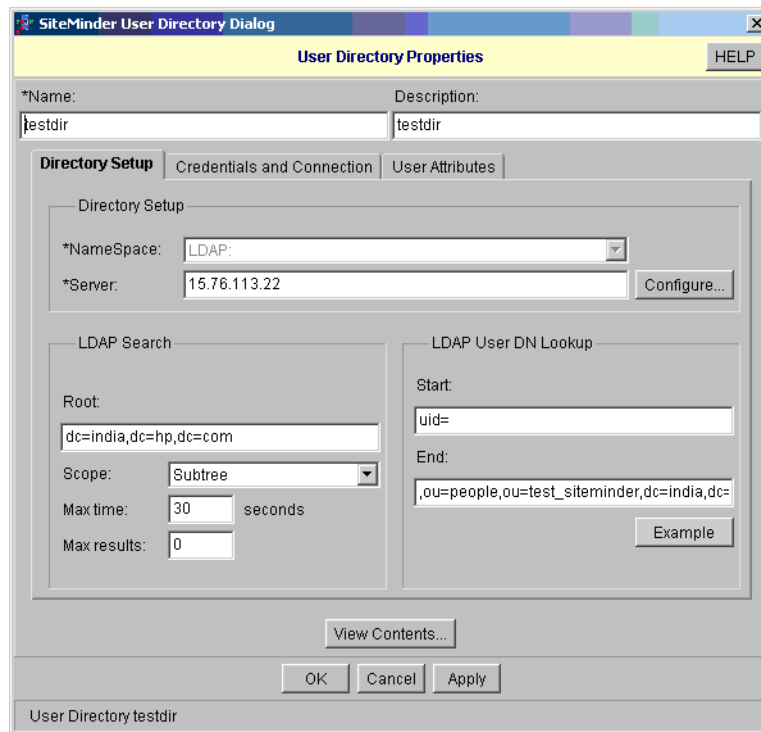
d   Configure the Credentials and Connection tab as shown here:

SiteMinder User Directory Dialog

User Directory Properties   HELP

*Name: Description:
testdir   testdir

Directory Setup   **Credentials and Connection**   User Attributes

Administrator Credentials

☑ Require Credentials   *Username: cn=Directory Manager
*Password: ********
*Confirm Password: ********

☑ Run in Authenticated User's Security Context

☐ Secure Connection

View Contents...

OK   Cancel   Apply

User Directory testdir

e   Configure the User Attributes tab as shown here:

SiteMinder User Directory Dialog

User Directory Properties   HELP

*Name: Description:
testdir   testdir

Directory Setup   Credentials and Connection   **User Attributes**

These are the names of directory user profile attributes SiteMinder
will use. These attributes must be available in the directory and
must not be used by any other application. Attributes marked R must
be readable; attributes marked RW must be read-write.

Universal ID (R):
Disabled Flag (RW):   nsaccountlock
Password Attribute (RW):   userpassword
Password Data (RW):
Anonymous ID (RW):
EMail (R):
Challenge/Response (RW):

View Contents...

OK   Cancel   Apply

User Directory testdir

For troubleshooting connectivity and configuration of the Policy Server, WebAgent, and LDAP
User Store, execute the sample Java programs that are provided with the SiteMinder SDK.
View the log files for details. The return code and error message may help to troubleshoot any
issue that might arise.

4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the SiteMinder connector with Select Identity and the connector specific parameters that you must provide while configuring the connector with Select Identity.

Configuration Procedure

After you deploy the connector RAR on application server, you must configure the connector with Select Identity. Perform the following steps to configure the SiteMinder connector with Select Identity.

1   Add a New Connector

2   Add a New Resource

3   Map Attributes

Add a New Connector

Add a new connector in Select Identity by using the user interface. While adding the connector, do the following:

- In the Connector Name text box, specify a name for the connector.

- In the Pool Name text box, enter **eis/**NetSm.

- Select No for the Mapper Available section.

Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on adding a new connector in Select Identity.

Add a New Resource

Add a new resource in Select Identity that uses the newly added connector. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instructions on adding a resource in Select Identity.

Refer to the following table while entering the parameters in the Basic Information and the Access Information pages:

Table 5   Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
Resource Name	SiteMinder	Name given to the resource.	
Connector Name	SiteMinder	The newly deployed connector.	Known as Resource Type on Select Identity 3.3.1.
Authoritative Source	No	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. You must specify **No** because the connector cannot synchronize account data with the Select Identity server.	
Associate to Group	Selected	Whether the system uses the concept of groups. For this connector, select this option.	Applicable only on Select Identity 3.3.1.
SiteMinder Admin	SiteMinder	SiteMinder superuser account name.	
Admin Password	Admin123	SiteMinder superuser password.	
SiteMinder User Directory	SiteMinder LDAP_User_Store	Name of the user directory as configured in SiteMinder.	
SiteMinder Root Organizational Unit	ou=smtesting	The name of the node in the LDAP user store. (Additional OUs are provided below this level.)	
OrgUnit Object Class	top, organizationalunit	Object class of the Org Unit in LDAP user store.	
Group Object Class	top, groupofuniquenames	Object class of the groups in LDAP user store.	
Group Suffix	ou=Groups	Group suffix name. This is one level below the "SiteMinder Root Organizational Unit" in the LDAP user store.	

Table 5   Resource Configuration Parameters (cont'd)

Field Name	Sample Values	Description	Comment
User Object Class	top, person, organizationalperson, inetorgperson	Object class of the user entry in LDAP user store.	
User Suffix	ou=People	User suffix name. This is one level below the "SiteMinder Root Organizational Unit" in the LDAP user store.	
Mapping File	netsm.xml	The attribute mapping XML file.	

*Instead of creating an authoritative resource, you can create authoritative attributes (in the next step) for the attributes that will be synchronized. Entitlements are authoritative by default in a non-authoritative resource but other attributes are not.

Map Attributes

After successfully adding a resource for the SiteMinder connector, you must map the resource attributes to Select Identity attributes. Refer to the *HP Select Identity Connector Deployment Guide* for information on mapping and creating attributes. While mapping attributes, refer to the following table for resource specific mapping information.

Table 6   SiteMinder Mapping Information

Select Identity Resource Attribute	Connector Attribute	SiteMinder Attribute	Description
User Name	Username	uid	Unique field
Password	Password	userpassword	User's password
First Name	Firstname	givenname	First name
Last Name	Lastname	sn	Surname
Email	Email	mail	Email ID
Common Name	Firstname	cn	Common name
AccountLockStatus	AccountLockStatus	nsaccountlock	The default value provided in the mapping file

Create the `AccountLockStatus` attribute on Select Identity. This attribute is used internally by the connector to enable or disable the user in the SiteMinder LDAP user store. If a user is disabled, he or she cannot log in to the Sun ONE directory resource. The mapping file contains an attribute called `nsaccountlock` to which you have to map this attribute. Refer to *Service Studio* chapter of *HP Select Identity Administration Online Help* for information adding a new attribute to Select Identity.

After mapping the attributes, you can use the connector to create a service, or you can associate the connector with an existing service. Refer to the *Service Studio* chapter of the *HP Select Identity Administration Online Help* for information on Select Identity services.

- The `nsaccountlock` attribute should not be included in the Service attributes. It is for internal use by the connector and should be specified in the resource attribute mappings.

- Do not add the `AccountLockStatus` attribute to any Service view; it is for internal use by the connector.

5 Uninstalling the Connector

If you want to uninstall a connector from Select Identity, perform the following steps:

- Remove all resource dependencies.
- Delete the connector from Select Identity.
- Delete the connector from application server.

See *HP Select Identity Connector Deployment Guide* for more information on deleting the connector from application server and Select Identity.

A Sample Images

This chapter illustrates some sample screenshots of Select Identity when SiteMinder connector in deployed on it.

- Select Identity 4.0-4.01 displays the Resource Access Information page in the following format, when a SiteMinder resource is deployed on it.

SiteMinder Resource: Resource Access Information

Modify the fields below as necessary and click Apply.

*Required Field ***

Siteminder Admin: *	SiteMinder
Admin Password: *	***********
Siteminder User Directory: *	testdir
Siteminder Root Organizational unit: *	ou=test_siteminder
OrgUnit Object Class:	top,organizationalUnit
Group Object Class: *	top,groupofuniquenames
Group Suffix: *	ou=Groups
User Object Class: *	top,person,organizationalPerson,inetorgperson
User Suffix: *	ou=People
Mapping File: *	netsm.xml (View)

- Select Identity 4.0-4.01 displays the View Attribute page in the following format, when a SiteMinder resource is deployed on it and resource attributes are mapped to Select Identity 4.0-4.01.

Attribute Mapping for SiteMinder Resource

Modify the fields below as necessary and click Apply.

Resource Attribute	Attribute	Sync In	Sync Out
[AccountLockStatus]	AccountLockStatus	false	false
[Email]	Email	false	false
[FirstName]	FirstName	false	false
[LastName]	LastName	false	false
[Password]	Password	false	false
[UserName]	UserName	false	false
SiteMinder Resource_ENTITLEMENTS	SiteMinder Resource_ENTITLEMENTS	true	true
SiteMinder Resource_KEY	SiteMinder Resource_KEY	true	true

- Select Identity 3.3.1 displays the Resource Access Information page in the following format, when a SiteMinder resource is deployed on it.

Resource Access Information	
* Resource Name:	SiteMinderResource
* Siteminder Admin:	SiteMinder
* Admin Password:	********
* Siteminder User Directory:	testdir
* Siteminder Root Organizational unit:	ou=test_siteminder
OrgUnit Object Class:	top,organizationalUnit
* Group Object Class:	top,groupofuniquenames
* Group Suffix:	ou=Groups
* User Object Class:	top,person,organizationalPerson,inetorgperson
* User Suffix:	ou=People
* Mapping File:	netsm.xml

- Select Identity 3.3.1 displays the Map Attribute page in the following format, when a SiteMinder resource is deployed on it and resource attributes are mapped to Select Identity 3.3.1.

Resource Attribute	MinLength	MaxLength	Mapped To	Authoritative
SiteMinderResource_ENTITLEMENTS	1	255	SiteMinderResource_ENTITLEMENT:	☑
SiteMinderResource_KEY	1	255	SiteMinderResource_KEY	☑
[AccountLockStatus]	1	64	AccountLockStatus	☐
[Email]	1	64	Email	☐
[FirstName]	1	64	FirstName	☐
[LastName]	1	64	LastName	☐
[Password]	1	64	Password	☐
[UserName]	1	64	UserName	☐